UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/800,181	03/12/2004	Kyung-Hee Lee	678-1395	8617

66547 7590 09/25/2007
THE FARRELL LAW FIRM, P.C.
333 EARLE OVINGTON BOULEVARD
SUITE 701
UNIONDALE, NY 11553

EXAMINER	
BAYOU, YONAS A	
ART UNIT	PAPER NUMBER
2134	

MAIL DATE	DELIVERY MODE
09/25/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)
	10/800,181	LEE ET AL.
	Examiner	Art Unit
	Yonas Bayou	2134

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *06 August 2007*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,3,6,7,12,14-16,32-34,42,46,47 and 64-67* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,3,6,7,12,14-16,32-34,42,46,47 and 64-67* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *12 March 2004* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *08/04/2006 and 07/28/2004*.

4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application

6) ☐ Other: _____.

DETAILED ACTION

1. This office action is in response to applicant's response filed on 08/06/2007.

2. Claims 1, 3, 6, 7, 12, 14-16, 32-34, 42, 46, 47 and 64-67 are pending.

3. Claims 2, 4, 5, 8-11, 13, 17-31, 35-41, 43-45 and 48-63 are cancelled.

4. Claims 1, 3, 6, 7, 12, 14-16, 32-34, 42, 46 and 47 are amended.

5. Claims 64-67 are added claims (New Claims).

6. Applicant's arguments have been fully considered.

Claim Objections

1. Claim 12 is objected to because of the following informalities:

claim 12 is a duplicate of claim 7.

Appropriate correction is required.

Examiner treats claim 12 as claim 7 for examination purpose.

Claim Rejections - 35 USC § 102

1. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

2. Claims 1, 3, 6, 7, 12, 14-16, 32-34, 42, 46, 47 and 64-67 are rejected under 35 U.S.C. 102(b) as being anticipated by Oberman et al, US Pub. No. 2001/0023425 A1 (hereinafter Oberman).

Referring to claim 1, Oberman teaches a signal processing apparatus for performing modular multiplication for use in a signal processing system, the apparatus comprising:

a first logic for outputting a signed multiplicand by selectively performing a one's complementary operation on a multiplicand according to a Booth conversion result of a multiplier in modular multiplication **[paragraph 103, lines 1-8, paragraph 104, lines 9-14 and fig. 7]**;

a second logic for outputting a modulus which is signed in the modular multiplication based on a carry input value Carry-in of a current clock, determined from a carry value cin for correction of a previous clock, and on a sign bit of the multiplicand **[paragraph 128, lines 8-16, paragraph 130 and fig. 16]**; and

a third logic for receiving the signed multiplicand and the signed modulus **[paragraph 143, lines 14-18 and fig. 19]**, and calculating a result value of the modular multiplication by iteratively performing a full addition operation on a carry value C and a sum value S of the full addition operation, found at the previous clock **[paragraph 130, lines 10-18, paragraph 131 and fig. 16]**.

Referring to claims 3 and 33, Oberman teaches a signal processing apparatus for performing modular multiplication for use in a signal processing system, wherein the first logic receives two least significant bits of the multiplier and a predetermined reference bit while sequentially shifting bits of the multiplier, and performs the Booth conversion thereon **[paragraph 98, lines 13-20 and paragraph 99]**.

Referring to claims 6, 34, 64 and 67, Oberman teaches a signal processing apparatus for performing modular multiplication for use in a signal processing system, wherein the first logic comprises:

a Booth conversion circuit for performing the Booth conversion using the two least significant bits of the multiplier and the reference bit **[paragraph 98, lines 13-20]**;

a multiplexer for multiplexing the multiplicand based on the two least significant bits of the multiplier **[paragraph 20, lines 13-19 and paragraph 104, lines 8-12]**; and

a one's complementer for outputting the signed multiplicand by selectively performing the one's complementary operation on the output of the multiplexer based on a sign bit of the Booth conversion result **[paragraph 103, lines 1-8, paragraph 104, lines 8-14 and fig. 7]**.

Referring to claims 7 and 65, Oberman teaches a signal processing apparatus for performing modular multiplication for use in a signal processing system, wherein the third logic performs the full addition operation using at least two Carry Save Adders

(CSAs) each including a plurality of full adders **[paragraph 25, paragraph 128 and fig. 16]**.

Referring to claim 14, Oberman teaches a signal processing apparatus for performing modular multiplication for use in a signal processing system, wherein the second logic comprises:

a quotient logic for determining at every clock first bit values which are extracted by as many values as a predetermined number of bits, beginning from a least significant bit for each of the carry value and the sum value calculated in the third logic, and second bit values for determining a multiple of modular reduction in the modular multiplication based on the carry input value Carry-in and a sign bit of the multiplicand **[paragraph 146 and 147]**; and

a selector for selecting the signed modulus based on the second bit values **[paragraph 13, lines 12-16]**.

Referring to claims 15 and 42, Oberman teaches a signal processing apparatus for performing modular multiplication for use in a signal processing system, wherein the third logic further comprises a full adder for outputting the carry input value Carry-in by performing the full addition operation using the carry value cin for correction and the sign bit of the multiplicand, received from the second logic **[paragraph 130, lines 10-18, paragraph 131 and fig. 16]**.

Referring to claims 16 and 46, Oberman teaches a signal processing apparatus for performing modular multiplication for use in a signal processing system, wherein the third logic performs a carry propagation addition operation on the carry value and the sum value output from the third logic after (m+2) clocks, where m=n/2, when each of the multiplier, the multiplicand and the modulus has n bits **[paragraph 135].**

Referring to claims 32 and 47, Oberman teaches a signal processing apparatus for performing modular multiplication for use in a signal processing system, wherein the third logic adds the modulus to the carry propagation addition operation result when a result of the carry propagation addition operation is a negative number **[paragraph 103, lines 15-18]**.

A signal processing method for performing modular multiplication for use in a signal processing system, the method comprising:

outputting a signed multiplicand by selectively performing a one's complementary operation on a multiplicand according to a Booth conversion result of a multiplier in modular multiplication **[paragraph 103, lines 1-8, paragraph 104, lines 9-14 and fig. 7]**;

finding a carry input value Carry-in of a current clock determined from a carry value cin for correction of a previous clock **[paragraph 213 and fig. 32]**;

outputting a modulus which is signed in the modular multiplication based on the carry input value and a sign bit of the multiplicand **[paragraph 128, lines 8-16 and fig. 16]**; and

receiving the signed multiplicand and the signed modulus **[paragraph 143, lines 14-18 and fig. 19]**, and calculating a result value of the modular multiplication by iteratively performing a full addition operation on a carry value C and a sum value S of the full addition Operation, found at the previous clock **[paragraph 130, lines 10-18, paragraph 131 and fig. 16]**.

Referring to claim 66, Oberman teaches a signal processing apparatus for performing modular multiplication for use in a signal processing system, wherein the outputting a signed modulus comprises:

extracting, at every clock, as many first bit values as a predetermined number of bits beginning from a least significant bit for each of the carry value and the sum value **[paragraph 146 and 147]**;

outputting second bit values for determining a multiple of modular reduction in the modular multiplication based on the first bit values, the carry input value Carry-in and a sign bit of the multiplicand **[paragraph 146 and 147]**; and

selecting the signed modulus based on the second bit values **[paragraph 13, lines 12-16]**.

Conclusion

3. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Yonas Bayou whose telephone number is 571-272-7610. The examiner can normally be reached on m-f,7:30-5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kambiz Zand can be reached on 571-272-3811. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

KAMBIZ ZAND
SUPERVISORY PATENT EXAMINER

Yonas Bayou

YB